La tutela della salute e della sicurezza nella scuola

di Pietro Boccia

Per quanto concerne l'igiene e la sicurezza nelle istituzioni scolastiche, bisogna partire con una riflessione sull'art. 32 della Costituzione repubblicana italiana che afferma: "La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività". La salute è, pertanto, individuale e collettiva. A livello individuale, è un diritto fondamentale e inalienabile, sancito costituzionalmente. A livello sociale, è un interesse collettivo, giacché le spese sanitarie e le ore di assenza dal lavoro sono a carico della collettività. Il D.Lgs. n. 626 ha, perciò, responsabilizzato i datori di lavoro e, di conseguenza, anche i Dirigenti scolastici. In ogni scuola, il Dirigente deve scegliere il Responsabile del servizio di prevenzione e protezione (RSPP) per effettuare la valutazione dei rischi e predisporre il documento sulla sicurezza e il piano di eventuali emergenze. Come controparte, la "626" prevede, anche in rappresentanza degli alunni, in alcuni casi equiparati ai lavoratori, il Rappresentante dei lavoratori per la sicurezza (RLS). Per quanto concerne la tutela della salute e della sicurezza nei luoghi di lavoro, sono obbligatori i corsi di formazione nelle istituzioni scolastiche; essi, però, per legge devono essere svolti al di fuori dall'orario di servizio. La normativa è, a tal proposito, indiscutibile e, pertanto, non si raccorda con l'orario di lavoro del docente. Ai sensi dell'art. 37, comma 12, del D.Lgs. n. 81/2008 riguardante la tutela della salute e della sicurezza nei luoghi di lavoro, la formazione deve, al contrario, svolgersi durante l'orario di lavoro, non potendo comportare oneri a carico dei lavoratori. Il Dirigente scolastico (art. 55, comma 4, lett. e) è obbligato "ad adempiere gli obblighi di formazione, d'informazione e di addestramento del corpo docente sul tema della sicurezza". Inserire la formazione dei docenti sulla sicurezza nell'orario di lavoro è, tuttavia, una contraddizione, perché essa non può essere svolta a discapito delle lezioni né inserita in ore di sospensione del servizio. In quest'ultimo caso, il docente non risulterebbe in servizio e ci sarebbe un palese conflitto con il comma 12 dell'art. 37 del Decreto legislativo n. 81/2008. La formazione sulla sicurezza non rientra nemmeno nelle attività obbligatorie che il docente è tenuto a prestare in base al comma 2 dell'art. 29 del Contratto collettivo. Allora come uscirne? Si potrebbe, secondo me, superare tale contraddizione soltanto se il Dirigente scolastico fosse in possesso di un alto profilo professionale e, dunque, capace di disciplinare la materia attraverso la contrattazione d'istituto. La sicurezza nei luoghi di lavoro, innervata nella Costituzione, deve essere immaginata come un insieme di misure sia di prevenzione sia di protezione che, a livello tecnico, organizzativo e procedurale, si stabiliscono e si attuano. Tali misure devono essere osservate non solo dal datore di lavoro o da chi lo rappresenta legalmente, ma anche dagli specialisti competenti (medici) e dagli stessi lavoratori all'interno delle strutture di lavoro. Quindi, la sicurezza sui luoghi di lavoro ha, da un lato, lo scopo di migliorare le condizioni lavorative di tutti coloro che operano all'interno delle strutture di lavoro e, dall'altro, quello di salvaguardare, in generale, la popolazione e l'ambiente. Essa , in Italia, è regolamentata dal Testo unico per la sicurezza sul lavoro (D.Lgs. n. 81/2008 – attuazione dell'art. 1 della L. 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro), e dalle disposizioni correttive del D.Lgs. n. 106/2009. Naturalmente la sicurezza deve essere salvaguardata anche in rete. La sicurezza in rete è, in generale, l'assenza in un sistema informatico delle condizioni conflittuali atte ad arrecare danni rilevanti o irreparabili ad un insieme di risorse, di informazioni e di dati. Essa è un settore dell'informatica che riguarda non solo il rischio, la vulnerabilità e le minacce dei dati ricevuti e trasmessi in una comunicazione con gli utenti, ma anche la

protezione del software (integrità logico-funzionale) di un sistema operativo. La sicurezza in rete si realizza attraverso misure organizzative e tecnologiche, che permettono di preservare il sistema e di proteggere la privacy degli utenti. Il Codice della privacy (D.Lgs. n. 196 del 30 giugno 2003, più volte modificato negli anni successivi) e il trattamento dei dati personali nei servizi di comunicazione elettronica sono connessi alla fornitura di servizi di tale comunicazione, che sono accessibili sulle reti pubbliche delle comunicazioni. È vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per attingerne informazioni o per monitorarne le operazioni. Il Codice deontologico individua i presupposti e i limiti entro i quali l'uso della rete - per determinati scopi legittimi e relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o per fornire uno specifico servizio richiesto dall'abbonato o dall'utente - è consentito, di norma, al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso in conformità ad una previa informativa che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento (art. 122 dl Codice). I dati che si riferiscono al traffico, ad abbonati e a utenti, trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica, che è accessibile al pubblico, vengono cancellati o resi anonimi nel momento in cui non sono più necessari ai fini della trasmissione della comunicazione elettronica. Nelle società attuali, giacché l'informazione è un bene immateriale che incorpora valore aggiunto, le istituzioni dovrebbero essere fortemente impegnate a garantire la privacy dei propri lavoratori e la sicurezza dei propri dati. Per tale motivo, esse, tra i tanti obblighi, dovrebbero assumere quello di redigere, annualmente, un documento programmatico sul modello approvato a livello internazionale dallo Standard ISO 27001:2005 (aggiornato alla versione 2013); tale documento dovrebbe prefiggersi la finalità di uniformare le modalità sia per proteggere le informazioni e i dati dalle minacce e dai danni sia per assicurare la privacy, l'integrità e la riservatezza di ciascuno. E' da tener presente, inoltre, che nel 2011 è entrato in vigore, nel campo della comunicazione, il Codice di autodisciplina. Questo è stato riproposto con poche variazioni e, in parte, modificato il 27 marzo 2014, quando è entrata in vigore, con il nuovo articolo 12, una norma disciplinare sulla comunicazione, contenente rivendicazioni ambientali (*green claims*).